REMARKS

Claims 1-15 stand rejected under 35 U.S.C. § 102(b) and § 103(a). Applicants have amended Claims 1, 6, and 7 to more particularly describe the invention. Applicants have added new Claims 16-26. Accordingly, Claims 1-26 are now pending in this application. Applicants request reconsideration of the rejections in view of the amendments and the following remarks.

Rejection of Claims 7 and 15

The Office Action rejected Claims 7 and 15 under 35 U.S.C. § 102(b) as being anticipated by Shwed, US Patent No. 5,606,668 (Shwed). Specifically, The Office Action stated that Shwed teaches a method for controlling e-mail message transmission across and e-mail firewall that is interposed between an internal network and an external network by intercepting a message and examining message content according to filter conditions in Col. 1, ll. 59-67 and Col. 2, ll. 1-60.

Applicants disagree with the Office Action that Shwed teaches a method for controlling e-mail messages. Rather, Shwed is only applicable to the inspection of packet level data. Specifically, Shwed discloses a system for examining information that "flows on the network in the form of packets." Col. 3, l. 66. Yet, Claim 7 recites "intercepting a **message**" and "filtering the **message**", as opposed to applying these operations to individual packets. Moreover, Shwed makes the specific distinction between its system and other systems operating on different levels in the ISO communication protocol model: "the packet filter of the invention intercedes between this level and level 3 which is the network software." Col. 7, ll. 5-7. According to Shwed, "an application (Level 7) may not be able to identify the source computer for a communication attempt (Levels 2-3), and therefore, may not be able to provide sufficient security." Col. 6, ll. 61-64.

Furthermore, examination of an individual packet of network data does not provide sufficient information regarding a message so as to allow Shwed to examine content associated with the message, as recited by Claim 7. Specifically, as is known in the art, each message is composed of several packet transmissions. The system of Shwed cannot examine the content of an entire message by only having data associated with a single packet. The system of Shwed does not remember data from previous packets, when looking at the current packet, so as to allow for interpreting high level message

information, which is usually spread across several packets of data. That is, there is no accumulation of packet data, which would allow for examining a message body, for example, or even reading header information. Hence, Shwed does not inspect a "message," which contains application level information, but only a packet of data which contains lower level protocol information.

As another example, a message sender or recipient identifier cannot be ascertained from individual packets because these identifier fields correspond to data encoded as message content, as opposed to the packet level source or destination information which is provided with a received packet as the physical, or network level, source and destination. In other words, a packet source or destination is not the same as an e-mail message sender and recipient. For example, a packet source is the network node where the packet is transmitted from. On the other hand, an e-mail message sender is the information encoded in an e-mail message, which identifies the user or application from which the e-mail message originated. Moreover, when an e-mail relay is used to serve several users in an enterprise, all packets associated with any user e-mail message arrive from the same source e-mail relay. When intermediate relays are employed to deliver packets of a message, the source of a packet is the intermediate relay rather than the sender address relevant to the present invention.

For example, to block email in the system of Shwed one would need to block using the low level information available at the packet level, i.e., source or destination IP address and port of an email server. Thus, Shwed could not reliably block e-mail messages from an e-mail service such as yahoo.com because 1) the IP address of the yahoo.com e-mail server cannot be used to control packets since it may change anytime and 2) there may be any number of low-level network gateways, firewalls, and routers in between the e-mail server and the system of Shwed. On the other hand, the system of Claim 7 does not refer to low level network information such as IP and port but rather is able to interpret higher level information, above the protocol level.

Shwed is not capable of applying a routing policy to a message since it operated on individual packets. As may be appreciated, even if proper data is provided by a single packet to allow for routing, as is recited by Claim 15, the remaining packets of the message, which may not include the allowable data, will be rejected, thereby leading to

an undesirable result where different portions of a single message are treated differently by the filtering system.

Hence, it may be appreciated that there is a fundamental difference between operation on the packet level and operation at the application level, as discussed by Shwed. Therefore, Shwed does not disclosed the application level message filtering and message transmission restricting as recited by Claims 7 and 15. Accordingly, Claims 7 and 15 are allowable over Shwed.

Rejection of Claims 1-6

The Office Action rejected Claims 1-6 under 35 U.S.C. § 103(a) as being unpatentable over Landfield, U.S. Patent No. 5,632,011 (Landfield), Bruce Schneier: Applied Cryptography 2nd edition, Oct. 1995 (Schneier), and Official Notice taken. Specifically, with respect to Claim 1, the Office Action stated that Landfield discloses intercepting a message from a sender to a recipient, searching an encryption directory for an encryption key and encrypting the message prior to allowing the message to pass through the firewall. With respect to Claim 6, the Office Action stated that Landfield discloses intercepting the message by the second e-mail firewall, decoding the message, and allowing the message to proceed to proceed to the recipient. Applicants note that the Office Action did not specify where Landfield discloses these features of Claim 6. Applicants respectfully disagree with the Office Action that Landfield discloses intercepting a message and encrypting a message with an encryption key of a firewall associated with the recipient. Applicants also disagree with the Office Action that Landfield discloses intercepting an e-mail message by an e-mail firewall of the recipient and decrypting the message before allowing it to proceed to the recipient.

Landfield does not disclose intercepting a message intended for a recipient associated with a second e-mail firewall. Rather, Landfield constructs, encrypts, and sends the e-mail message at the sending firewall. Col. 4, ll. 3-6. There is no interception of an e-mail message in Landfield. The message of Landfield is constructed and encrypted by the sender server, not by an e-mail firewall that intercepted the message, as recited by Claims 1-5. Moreover, Landfield does not employ an encryption key of an e-mail firewall of the recipient, since the recipient and e-mail firewall in Landfield are the same. As may be appreciated, an e-mail firewall that is the recipient of a message does

not provide the function of a firewall for itself. Claims 1-5 clearly recite that the recipient and the e-mail firewall are two different entities, otherwise the term "intercepting" would become insignificant, as a recipient receiving a message addressed to it cannot be said to have "intercepted" the message.

Applicants further disagree with the Office Action that the use of a public and private key pair for encryption and decryption of user messages by an e-mail firewall, which is outside the user control, is old and well known. Such facts are not suitable for official notice as they are not capable of instant and unquestionable demonstration as being "well-known" in the art. *In re Ahlert*, 424 F.2d 1088, 1091 (CCPA 1970). Specifically, Claims 1-5 recite that the e-mail control system encrypts e-mail messages intended for an individual user using an encryption key of the recipient e-mail firewall rather than an encryption key of the recipient. Applicants submit that none of the prior art references cited, nor the state of the applicable field of art, as of the date of invention, disclose employing a firewall level key for encrypting messages, which are intended for users associated with the firewall. Therefore, Claims 1-5, as well as new Claim 25 are allowable over the prior art for at least this reason alone.

Rejection of Claims 8-14

Claims 8-14 all depend from Claim 7. As discussed above, Claim 7 is allowable. Accordingly, Claims 8-14 are allowable by at least their depending from allowable Claim 7.

New Claims 16-26

Applicants have added new Claims 16-26. The new claims are fully supported by the specification as filed. Accordingly, no new matter is added.

New independent Claims 16, 17, 18, and 24 recite that the e-mail firewall transmits an e-mail message to a recipient address in response to a predetermined policy result. Neither Landfield nor Shwed, or the prior art in general, disclose such transmitting of an e-mail message to a recipient address in response to application of a policy. Therefore, Claims 16, 17, 18 and 24 are allowable over Landfield and Shwed for at least this reason alone.

Claims 19-23 include the base claim limitations of independent Claim 18. As discussed above, Claim 18 is allowable over the prior art. Therefore, Claims 19-23 are allowable over the prior art for at least this reason alone.

New Independent Claim 25 recites first and second e-mail firewalls, each intercepting e-mail messages from and to a local e-mail server. The first firewall encrypts messages intercepted from its corresponding e-mail server, while the second e-mail firewall decrypts messages intercepted on their way to its corresponding e-mail server. As discussed above with respect to Claims 1-6, the prior art does not disclose such interception and encryption by an email firewall. Landfield discloses a firewall system that composes, encrypts, and sends an e-mail message addressed to a second firewall system. Col. 4, ll. 3-8. Landfield does not intercept a message from an e-mail server but rather composes the e-mail message and initiates transmission at the firewall. As may be appreciated by one skilled in the art, the flow is the opposite of that of the system recited by Claim 25, since the first firewall system of Landfield likely employs an e-mail server to route the message to the second firewall system. Therefore, as discussed above, Landfield does not disclose intercepting an e-mail message as recited by Claim 25. Thus, Claim 25 is allowable over Landfield for at least this reason alone.

Claim 26 includes the base claim limitations of independent Claim 25. As discussed above, Claim 25 is allowable over Landfield. Therefore, Claim 26 is allowable over Landfield.

SUMMARY

In view of the forgoing supporting remarks, Applicants respectfully request allowance of pending Claims 1-26. This application is now believed to be in a condition for allowance.

If the Examiner wishes to direct any questions concerning this application to the undersigned Applicants' representative, please call the number indicated below.

Dated: June 30, 2003

Respectfully submitted,

Guy Perry
Reg. No. 46,194

Attorney for Applicant
(212) 735-3000
Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036

MARKED UP CLAIMS

1. A method for transmitting a message between a sender user associated with a first e-mail firewall and a recipient user associated with a second e-mail firewall, the method comprising:

intercepting a message from the sender user intended for the recipient user;

searching an encryption directory for an entry associated with the second e-mail firewall associate with the recipient user;

retrieving an encryption key associated with the[a] second e-mail firewall, the second e-mail firewall associated with a plurality of [the] recipient users;

encoding the message with the encryption key of the second e-mail firewall to provide an encrypted message; and

allowing the message to proceed to said recipient user [through the firewall].

6. A method for receiving a message by a recipient user associated with a second e-mail firewall from a sender user associated with a first e-mail firewall, the first e-mail firewall encoding the message by using an encryption key of the second e-mail firewall, comprising:

intercepting the message by the second e-mail firewall, the second e-mail firewall associated with a pluraliry of recipient users;

decoding the message with a private key of the second e-mail firewall; and

allowing the message to proceed [through the firewall] to the recipient user.

7. A method for controlling e-mail message transmission across an e-mail firewall, the e-mail firewall interposed between an internal network and an external network[s], the method comprising:

[I]intercepting a message from a sender user associated with the internal network, the message directed to a recipient user associated with an external network;